SPECIFICATION AMENDMENTS

Please replace the paragraph [0018] with the following rewritten paragraph:

[0018] FIG. 1 shows the basic components of the authentication framework according to the present invention. Using the framework an end user is able to authenticate through a stacking mechanism. As shown in FIG. 1 a client 10 on log in sends a message such as an authentication domain ID to an authentication server 11. A server builds an authentication model stack configuration 12 which provides a profile of the client based on the authentication domain ID. Through the authentication stack the authentication server is able to seek authentication through either remote authentication modules 13, 13' or local authentication modules 14, 14'. Each time a user triggers the authentication service the server creates a new authentication stack. Each element in the stack refers either to a local or to a remote module. Some of the entries of the stack may have been configured such that they are unable to render an actual authentication service but in fact trigger an authentication component that is remotely deployed. The processing of this remote component will create the actual authentication context necessary to handle the user authentication process on a specific authentication device. The authentication devices may be one of various biometrics schemes or it may be a cryptographic hardware service or appliance or it could be a smart card, USB token etc. The main authentication process that sits on the authentication server consolidates the results that it gets back from all of the virtual stack entities. It combines the consolidated results with the stack entries bound to the local authentication modules in order to reconstitute the entire authentication stack.

Please replace the paragraph [0020] with the following rewritten paragraph:

[0020] First the client to be authenticated sends to the authentication server a so called authentication domain ID, shown in step 20. The authentication domain ID ~~that~~ could be, for example, an application service identifier. The authentication server builds the authentication stack according to the configuration defined by the specific ID~~.~~, as shown in steps 21, 22, 23, 24 and 25. Hence, a direct mapping must be explicitly defined on the authentication server to map an application ID with a list of software modules~~.~~, which is shown intuitively by database 50. An example of the configuration could be:

-Application1

RADIUSmodule

OSmodule

Application2

SMARTCARDmodule

OSmodule

KERBEROSmodule

Please replace the paragraph [0021] with the following rewritten paragraph:

[0021] At initiation of the authentication process each entry in the authentication stack is processed. If the entry is mapped to a local authentication module, branch "Yes" of decision block 23, the authentication process is performed locally~~.~~, by triggering the local authentication

module as shown in step 24. Otherwise, shown by branch "No" of decision block 23, the authentication server triggers a remote authentication module, step 26, which retrieves authentication data from its local authentication device~~.~~, step 27. The authentication server then checks the validity of the data, shown in step 28. Once all the stack entries have been processed, branch "Yes" of decision block 22, the authentication server consolidates the results~~.~~, shown in step 30. If the authentication is successful, branch "Yes" of block 31, a unique session identifier characterising the authentication session is sent back to the client~~.~~, step 32. Otherwise, branch "No" of decision block 31, the client is notified by the authentication server that the authentication process is failed~~.~~, step 33.

Please replace the paragraph [0023] with the following rewritten paragraph:

[0023] As shown in Figure 3 the client operator 10, 10' or 10" connects to the network management system 5620 NM (NMS) which runs the authentication server~~.~~ 11. This is shown intuitively by arrow denoted with 1 on Figure 3. The authentication server triggers the authentication module that sits on the client and this could be OS, USB-tokens, smartcards etc., arrow denoted with 2. It then triggers the Element Management System ~~(EMS)~~ authentication module 15, arrow 3, which may be running for example on an element management system 1353/EMS. Then ~~it would~~the authentication server 11 could trigger, arrows 4, 5, authentication modules 13, 13' that are running on the network element NE3 (or NE1, NE2) relaying the request to a remote authentication server 6 such as radius.

Please replace the paragraph [0024] with the following rewritten paragraph:

[0024] Figure 4 exemplifies a deployment use case of the authentication stack in the course of an authentication process. In this case the client authentication involves different steps. A dedicated authentication module that sits on the client 10 handles the operating system based authentication and retrieves OS credentials of the current logged in user. A server component 40 on authentication server 11 handles directly the RADIUS based authentication and a smartcard authentication module 41 handles authentication requests on the client side. The authentication module retrieves user credentials thanks to its direct access to the local smartcard reader appliance. 43. An LDAP (lightweight directory access protocol) module 44 that sits on a specific network element 43 handles the authentication requests and access to the LDAP backend is performed through a dedicated LDAP module.